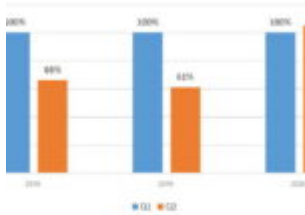
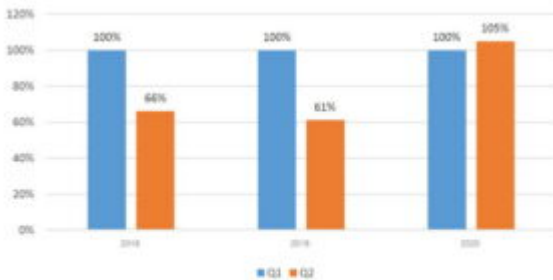


ยูสเซอร์ยกเลิกแผนการวันหยุด แต่โจรไซเบอร์ไม่มีวันหยุด แคสเปอร์สกีเผยตัวเลขการโจมตี DDoS เพิ่มขึ้น 3 เท่าจากปีก่อน



The difference between Q1 and Q2 through 2019-2020. Q1 of each year is taken as 100%.



The difference between Q1 and Q2 through 2018-2020. Q1 of each year is taken as 100%.

รายงานของแคสเปอร์สกี เรื่อง Kaspersky Q2 2020 DDoS Attacks Report เผยจำนวนการโจมตีโดย DDoS ในช่วงไตรมาสที่สองของปี 2020 เพิ่มขึ้นสามเท่าเมื่อเปรียบเทียบกับช่วงไตรมาสที่สองของปี 2019 โดยที่ตัวเลขเกือบจะเท่ากับจำนวนการโจมตีในไตรมาสที่หนึ่งของปี 2020 เลยทีเดียว ผู้เชี่ยวชาญของแคสเปอร์สกี เชื่อว่าการเพิ่มจำนวนเช่นนี้น่าจะมีส่วนมาจากการแพร่ระบาดของโควิด-19 เนื่องจากทั้งอาชญากรไซเบอร์และเหยื่อเป้าหมายต่างก็จำเป็นต้องวางแผนกิจกรรมช่วงนี้กันใหม่ทั้งสองฝ่ายนั่นเอง

การแพร่ระบาดของโควิด-19 ทั่วโลก และข้อกำหนดเรื่องระยะห่างทางสังคมนั้นเข้ามาเปลี่ยนแปลงวิถีชีวิตผู้คนอย่างใหญ่หลวง โดยเฉพาะอย่างยิ่ง หลายคนรู้สึกกังวลเกี่ยวกับการเดินทาง หรือไม่มีใจที่จะเดินทางได้ไปเสียง่ายๆ อย่างนั่นเอง ดังนั้น หลายคนหันมาอยู่กับบ้าน “staycation” หรือยกเลิกแผนการวันหยุด ซึ่งส่งผลที่คาดไม่ถึงหลายประการ และหนึ่งในนั้นคือ การเพิ่มจำนวนการคุกคามโจมตีของ DDoS

จำนวนการโจมตีตามที่ Kaspersky DDoS Protection ตรวจจับและบล็อกได้ในช่วงไตรมาสที่สองของปี 2020 นั้นเพิ่มสูงขึ้นจากช่วงเวลาเดียวกันของปี 2019 ถึง 217% และยังเพิ่มขึ้นอีกในไตรมาสที่สองของปี 2020 อีกนิดหน่อยจากไตรมาสแรกของปี

ข้อมูลเหล่านี้ขัดแย้งกับทิศทางประจำปีที่นักวิจัยของแคสเปอร์สกีค้นคว้า โดยปกติ จำนวนของการโจมตีโดยใช้ DDoS นั้นต่างกันในแต่ละฤดูกาล เริ่มต้นปีเรามักจะได้พบเจอ DDoS เข้าโจมตีค่อนข้างเยอะ เนื่องจากเป็นช่วงเริ่มต้นเทศกาลธุรกิจของปี และช่วงเกือบกลางปีก็จะค่อยๆ ลดลง ตัวอย่างเช่น จำนวนการเข้าโจมตีในไตรมาสสองของปี 2019 ลดลง 39% เทียบกับไตรมาสแรกของปี 2019 และความต่างระหว่างสองไตรมาสของปี 2018 อยู่ที่ 34%

ทิศทางนี้เห็นผลสะท้อนได้ในจำนวนของคอมมานด์ที่บ็อตได้รับมาจาก C&C servers ซึ่งระบบข้อมูลวิเคราะห์ Kaspersky DDoS Intelligence System สกัดและวิเคราะห์ไว้ได้ โดยรวมแล้ว ตัวเลขเฉลี่ยของการโจมตีที่จับได้รายวันในช่วงไตรมาสที่สองนั้นเพิ่มขึ้นจากไตรมาสที่หนึ่งถึงเกือบ 30% และจำนวนการโจมตีที่สูงสุดต่อวันที่นับได้ถึงเกือบ 300 ครั้งในไตรมาสที่สอง (บันทึกเมื่อ 9 เมษายน) ขณะที่ไตรมาสที่หนึ่งของปี 2020 นับได้ 242 ครั้ง

อเล็กซี่ ไคเซเลฟ ผู้จัดการฝ่ายพัฒนาธุรกิจ ทีมป้องกันการคุกคามจาก DDoS ของแคสเปอร์สกี กล่าวว่า “ปีนี้ ผู้คนไม่สามารถใช้เวลาไปกับช่วงหน้าร้อนอันแสนสุขได้ตามปกติ จากมาตรการล็อกดาวน์ในหลายประเทศจากการแพร่ระบาดของ โควิด-19 เป็นเหตุให้ผู้คนมากมายหันมาพึ่งพากิจกรรมออนไลน์ ทั้งเรื่องส่วนตัวและการทำงาน ธุรกิจออนไลน์และแหล่งข้อมูลต่างเฟื่องฟูช่วงหน้าร้อนนี้ ผลคือ เราได้พบเห็นความเคลื่อนไหวบางประการในตลาด DDoS และยังไม่เห็นเหตุให้คาดการณ์ว่าจะลดการเคลื่อนไหวลงแต่อย่างใด”

เพื่อช่วยองค์กรในการป้องกันตัวเองให้พ้นจากการคุกคามของ DDoS ระหว่างช่วงวันหยุดนั้น แคสเปอร์สกีขอแนะนำมาตรการดังต่อไปนี้:

1. มอบหมายให้ผู้เชี่ยวชาญด้านกรับมือกับการคุกคาม DDoS ดูแลการใช้งานทรัพยากรบนเว็บ เตรียมตัวเพื่อรับมือกับเหตุการณ์นอกเวลาทำการ ช่วงเย็นถึงดึก และสุดสัปดาห์
2. ตรวจสอบความถูกต้องของข้อมูลและข้อมูลติดต่อกับเซิร์ฟเวอร์ รวมถึงผู้ให้บริการอินเทอร์เน็ต นี้จะช่วยให้ทีมงานสามารถติดต่อได้กรณีเกิดเหตุฉุกเฉิน
3. ติดตั้งโซลูชันระดับโปร ซึ่งสามารถป้องกันองค์กรให้พ้นจาก DDoS ได้ เช่น Kaspersky DDoS Protection ที่มีทั้งความเชี่ยวชาญที่สั่งสมมานานในการต่อสู้กับภัยไซเบอร์ และความรู้ที่พัฒนาขึ้นภายในองค์กรเอง

อ่านรายงานฉบับเต็มได้ที่ Securelist <https://securelist.com/ddos-attacks-in-q2-2020/98077/>